

# Iso-Orthogonality and Type-II Duadic Constacyclic Codes

Yun Fan and Liang Zhang

Dept of Mathematics, Central China Normal University, Wuhan 430079, China

## Abstract

Generalizing even-like duadic cyclic codes and Type-II duadic negacyclic codes, we introduce even-like (i.e., Type-II) and odd-like duadic constacyclic codes, and study their properties and existence. We show that even-like duadic constacyclic codes are isometrically orthogonal, and the duals of even-like duadic constacyclic codes are odd-like duadic constacyclic codes. We exhibit necessary and sufficient conditions for the existence of even-like duadic constacyclic codes. A class of even-like duadic constacyclic codes which are alternant MDS-codes is constructed.

*Keywords:* Finite field, constacyclic code, isometry, even-like duadic code, iso-orthogonal code.

*MSC2010:* 12E20, 94B60.

## 1 Introduction

The study of duadic cyclic codes was initiated by Leon, Masley and Pless [16], and attracted many attentions, e.g. [17, 19, 11, 12, 14]. The research on duadic cyclic codes over finite fields has greatly developed, see [15, Ch.6]. Rushanan [18] generalized duadic cyclic codes to the duadic group codes, and many results about the existence of such codes, especially the duadic abelian codes, were obtained, e.g. [20, 2].

Note that most of the studies on duadic cyclic codes over finite fields consider the semisimple case, i.e., the length of the codes is coprime to the cardinality of the finite field. In that case, duadic cyclic codes are not self-dual; the key obstruction is the 1-dimensional cyclic code with check polynomial  $X - 1$ , which is invariant by any multipliers. By appending with one bit, self-dual extended cyclic codes might be obtained. It is the same for group codes, more generally, for transitive permutation codes, see [13].

Another perspective to carry the research forward is to consider constacyclic codes. Let  $F_q$  be the finite field with  $q$  elements, where  $q$  is a power of a prime,

---

*Email addresses:* yfan@mail.ccnu.edu.cn (Y. Fan); 554701169@qq.com (L. Zhang).

let  $F_q^*$  be the multiplicative group consisting of the non-zero elements of  $F_q$ . Let  $n$  be a positive integer coprime to  $q$ , and  $\lambda \in F_q^*$  with  $r = \text{ord}_{F_q^*}(\lambda)$ , where  $\text{ord}_{F_q^*}(\lambda)$  denotes the order of  $\lambda$  in the group  $F_q^*$ . Any ideal  $C$  of the quotient algebra  $F_q[X]/\langle X^n - \lambda \rangle$  is called a  $\lambda$ -constacyclic code of length  $n$  over  $F_q$ , where  $F_q[X]$  denotes the polynomial algebra over  $F_q$  and  $\langle X^n - \lambda \rangle$  denotes the ideal generated by  $X^n - \lambda$ . In the following we always use the three numbers  $q, n, r$  to parametrize the  $\lambda$ -constacyclic code  $C$ . If  $r = 1$  (i.e.  $\lambda = 1$ ) then  $C$  is just a cyclic code. If  $r = 2$  (i.e.  $\lambda = -1$ ) then  $C$  is named *negacyclic code*.

Aydin *et al* [3] exhibited the BCH bound of constacyclic codes. Dinh *et al* [10, 9] studied constacyclic codes and showed that self-duality happens for (and only for) negacyclic codes.

Blackford [4, 5] contributed very much to the study of the duadic constacyclic codes. Let  $\mathbb{Z}_{nr}$  be the residue ring of the integer ring  $\mathbb{Z}$  modulo  $nr$ . The set of roots of the polynomial  $X^n - \lambda$  in its splitting field corresponds to a subset of  $\mathbb{Z}_{nr}$ :  $1 + r\mathbb{Z}_{nr} = \{1, 1 + r, \dots, 1 + r(n-1)\}$ . The multipliers act on this set  $1 + r\mathbb{Z}_{nr}$ . In this way, Blackford [4] obtained all self-dual negacyclic codes, introduced Type-I and Type-II duadic splittings in the negacyclic case (i.e.  $r = 2$ ), and proved the existence of Type-II duadic negacyclic codes for the case when  $n$  is even but  $n/2$  is odd. Further, in [5], it was shown that the Type-I duadic constacyclic codes are just the so-called *iso-dual* constacyclic codes.

Type-I polyadic (including duadic) constacyclic codes were studied in [7]. In terms of the Chinese Remainder Theorem, the set  $1 + r\mathbb{Z}_{nr}$  and the multiplier group can be decomposed suitably. Necessary and sufficient conditions for the existence of such codes were obtained. Some generalized Reed-Solomon or alternant constacyclic codes were constructed from Type-I polyadic constacyclic codes.

In this paper, generalizing even-like (Type-II) and odd-like duadic negacyclic codes, we introduce even-like (i.e., Type-II) and odd-like duadic constacyclic codes, and study their properties and existence.

In Section 2, necessary notations and fundamentals are described.

In Section 3, with isometries between constacyclic codes, even-like (i.e., Type-II) and odd-like duadic constacyclic codes are defined, and a relationship between the two kinds of duadic constacyclic codes are exhibited (Theorem 3.7 below). As known, even-like duadic constacyclic codes are not self-orthogonal in general. We show that they are *iso-orthogonal* and, up to some sense, they are the maximal iso-orthogonal pairs of constacyclic codes (Theorem 3.12).

For the existence of Type-I duadic constacyclic codes, a necessary and sufficient condition has been obtained in [7, Th.4], see Lemma 4.3(iii) below also. In Section 4, we present necessary and sufficient conditions for the existence of Type-II duadic constacyclic codes, see Theorem 4.1 below, where the cyclic case and the negacyclic case are included as straightforward consequences.

In Section 5, a class of alternant MDS-codes is constructed from even-like duadic constacyclic codes (Proposition 5.1), and some specific examples are presented.

## 2 Preliminaries

Throughout this paper,  $F_q$  is the finite field with  $q$  elements,  $\lambda \in F_q^*$  has multiplicative order  $r$ , and  $n$  is a positive integer that is relatively prime to  $q$ . Note that the order of the multiplicative group  $|F_q^*| = q - 1$ , hence  $r \mid (q - 1)$ . Following [5], we abbreviate the quotient algebra by

$$R_{n,\lambda} = F_q[X]/\langle X^n - \lambda \rangle. \quad (2.1)$$

If  $C$  is an ideal of  $R_{n,\lambda}$  (i.e., a  $\lambda$ -constacyclic code  $C$  over  $F_q$  of length  $n$ ), we say that  $C \subseteq R_{n,\lambda}$  is a  $\lambda$ -constacyclic code.

In this paper we always assume that  $\theta$  is a primitive  $nr$ -th root of unity (in a suitable extension of  $F_q$ ) such that  $\theta^n = \lambda$ . As mentioned in the Introduction, the set of roots of  $X^n - \lambda$  corresponds to the subset  $P_{n,\lambda}$  of the residue ring  $\mathbb{Z}_{nr}$ , which is defined by:

$$P_{n,\lambda} = 1 + r\mathbb{Z}_{nr} = \{1 + rk \pmod{nr} \mid k \in \mathbb{Z}_{nr}\}, \quad (2.2)$$

so that

$$X^n - \lambda = \prod_{i \in P_{n,\lambda}} (X - \theta^i).$$

By  $\mathbb{Z}_{nr}^*$  we denote the multiplicative group consisting of units of  $\mathbb{Z}_{nr}$ . The group  $\mathbb{Z}_{nr}^*$  acts on  $\mathbb{Z}_{nr}$  by multiplication. Precisely, any  $t \in \mathbb{Z}_{nr}^*$  induces a permutation  $\mu_t$  of the set  $\mathbb{Z}_{nr}$  as follows:  $\mu_t(k) = tk$  for all  $k \in \mathbb{Z}_{nr}$ . Any  $\mu_t$ -orbit on  $\mathbb{Z}_{nr}$  is abbreviated as a  $t$ -orbit. The set of  $t$ -orbits on  $\mathbb{Z}_{nr}$  (i.e., the quotient set by  $\mu_t$ ) is denoted by  $\mathbb{Z}_{nr}/\mu_t$ . For any subset  $P \subseteq \mathbb{Z}_{nr}$ , the permutation  $\mu_t$  transforms  $P$  to the subset  $tP = \{tk \pmod{nr} \mid k \in P\}$ . We say that  $P$  is  $\mu_t$ -invariant if  $tP = P$ . If  $t \equiv t' \pmod{r}$  with  $1 \leq t' < r$  (recall that  $t$  is coprime to  $r$ ), it is easy to see that

$$tP_{n,\lambda} = t + r\mathbb{Z}_{nr} = t + r\mathbb{Z}_{nr} = t' + r\mathbb{Z}_{nr} = t'P_{n,\lambda},$$

and  $\theta^j$  for  $j \in t' + r\mathbb{Z}_{nr}$  are the roots of  $X^n - \lambda^t = X^n - \lambda^{t'}$ . So we denote  $t + r\mathbb{Z}_{nr} = P_{n,\lambda^t}$ . With this notation, for any  $t \in \mathbb{Z}_{nr}^*$  we have

$$X^n - \lambda^t = \prod_{i \in P_{n,\lambda^t}} (X - \theta^i), \quad \text{where } P_{n,\lambda^t} = tP_{n,\lambda}. \quad (2.3)$$

Further, for any  $s \in \mathbb{Z}_{nr}^*$ , it is easy to see that  $sP_{n,\lambda^t} = P_{n,\lambda^t}$  if and only if  $s \in 1 + r\mathbb{Z}_{nr}$ , i.e.,  $s \in \mathbb{Z}_{nr}^* \cap (1 + r\mathbb{Z}_{nr})$ . We denote

$$G_{n,r} = \mathbb{Z}_{nr}^* \cap (1 + r\mathbb{Z}_{nr}), \quad (2.4)$$

which is a subgroup of the group  $\mathbb{Z}_{nr}^*$ . We call  $G_{n,r}$  the *multiplier group*.

Since  $r \mid (q - 1)$ , we see that  $q \in G_{n,r}$ . The  $q$ -orbits on  $\mathbb{Z}_{nr}$  are also named *q-cyclotomic cosets* (abbreviated to *q-cosets*) in literature, so we call them by

$q$ -cosets. Obviously,  $P_{n,\lambda^t} = t + r\mathbb{Z}_{nr}$  is  $\mu_q$ -invariant for any  $t \in \mathbb{Z}_{nr}^*$ . For any  $q$ -coset  $Q \in P_{n,\lambda^t}/\mu_q$ , the polynomial  $f_Q(X) = \prod_{i \in Q} (X - \theta^i)$  is irreducible in  $F_q[X]$ . Thus

$$X^n - \lambda^t = \prod_{Q \in P_{n,\lambda^t}/\mu_q} f_Q(X) \quad (2.5)$$

is the monic irreducible decomposition in  $F_q[X]$ .

For any  $\mu_q$ -invariant subset  $P$  of  $P_{n,\lambda}$ , We have a polynomial

$$f_P(X) = \prod_{Q \in P/\mu_q} f_Q(X) \in F_q[X].$$

Let  $\overline{P} = P_{n,\lambda} \setminus P$  (which denotes the difference set), i.e.,  $\overline{P}$  is the complement of  $P$  in  $P_{n,\lambda}$ . By (2.5),

$$f_P(X)f_{\overline{P}}(X) = X^n - \lambda. \quad (2.6)$$

**Remark 2.1.** It is well-known that for any  $\lambda$ -constacyclic code  $C \subseteq R_{n,\lambda}$  there is exactly one  $\mu_q$ -invariant subset  $P \subseteq P_{n,\lambda}$  such that, for any  $a(X) \in R_{n,\lambda}$ ,

- $a(X) \in C$  if and only if  $a(X)f_P(X) \equiv 0 \pmod{X^n - \lambda}$ ;
- $a(X) \in C$  if and only if  $f_{\overline{P}}(X) \mid a(X)$ .

The polynomial  $f_P(X)$  is said to be a *check polynomial* of the  $\lambda$ -constacyclic code  $C$ , while the polynomial  $f_{\overline{P}}(X)$  is said to be a *generator polynomial* of  $C$ . In that case we denote  $C = C_P$  and call it the  $\lambda$ -constacyclic code with *check set*  $P$  and *defining set*  $\overline{P}$  (which corresponds to the zeros of  $C_P$ ). It is easy to see that

$$C_P \subseteq C_{P'} \iff P \subseteq P', \quad \text{for } \mu_q\text{-invariant subsets } P, P' \subseteq P_{n,\lambda}; \quad (2.7)$$

which implies that

- *mapping a  $\lambda$ -constacyclic code of length  $n$  over  $F_q$  to its check set is an isomorphism from the lattice of  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  onto the lattice of  $\mu_q$ -invariant subsets of  $P_{n,\lambda}$ .*

Any element of  $R_{n,\lambda}$  has a unique representative:  $a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ . We always associate any word  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in F_q^n$  with the element  $a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in R_{n,\lambda}$ , and *vice versa*. For any  $a(X), b(X) \in R_{n,\lambda}$  associated to words  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}), \mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in F_q^n$ , the Hamming weight  $w(a(X))$  is defined by the Hamming weight of the word  $\mathbf{a}$ ; the Euclidean inner product of  $a(X)$  and  $b(X)$  is defined by the Euclidean inner product of the words  $\mathbf{a}$  and  $\mathbf{b}$ :

$$\langle a(X), b(X) \rangle = \langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=0}^{n-1} a_i b_i. \quad (2.8)$$

For  $C \subseteq F_q^n$ , denote

$$C^\perp = \{\mathbf{a} \in F_q^n \mid \langle \mathbf{c}, \mathbf{a} \rangle = 0, \forall \mathbf{c} \in C\},$$

which is called the (*Euclidean*) *dual code* of  $C$ . It is known that, for a  $\lambda$ -constacyclic code  $C$ , the dual code  $C^\perp$  is in fact a  $\lambda^{-1}$ -constacyclic code, see [4, 9], or see Lemma 3.5 below for more precise description.

**Remark 2.2.** Let  $\Gamma$  be a finite set, and  $\sigma$  be a permutation of  $\Gamma$ . We need the following group-theoretical results (cf. [7, Lemmas 6-8]). For fundamentals about groups, please refer to [1].

- (i) The group generated by  $\sigma$  is denoted by  $\langle \sigma \rangle$ . The orbits of  $\langle \sigma \rangle$  on  $\Gamma$  is abbreviated by  $\sigma$ -orbits. The length of the  $\sigma$ -orbit containing  $k \in \Gamma$  is equal to the index  $|\langle \sigma \rangle : \langle \sigma \rangle_k|$ , where  $\langle \sigma \rangle_k$  denotes the subgroup consisting of the elements of  $\langle \sigma \rangle$  which fix  $k$ . In particular, the length of any  $\sigma$ -orbit is a divisor of the order  $\text{ord}(\sigma)$  of  $\sigma$ .
- (ii) There is a partition  $\Gamma = \Gamma_1 \cup \Gamma_2$  such that  $\sigma(\Gamma_1) = \Gamma_2$  and  $\sigma(\Gamma_2) = \Gamma_1$  if and only if the length of every  $\sigma$ -orbit on  $\Gamma$  is even.
- (iii) Further assume that  $\sigma'$  is a permutation of a finite set  $\Gamma'$ , hence  $(\sigma, \sigma')$  is a permutation of the product  $\Gamma \times \Gamma'$ . Then the order of the permutation  $(\sigma, \sigma')$  is equal to the least common multiple of the order of  $\sigma$  and the order of  $\sigma'$ ; the length of the  $(\sigma, \sigma')$ -orbit containing  $(k, k') \in \Gamma \times \Gamma'$  is equal to the least common multiple of the length of the  $\sigma$ -orbit containing  $k \in \Gamma$  and the length of the  $\sigma'$ -orbit containing  $k' \in \Gamma'$ .
- (iv) Assume that a finite group  $G$  acts on a finite set  $\Gamma$  and  $N$  is a normal subgroup of  $G$ . Let  $\Gamma/N$  be the set of  $N$ -orbits on  $\Gamma$ , called the *quotient set* of  $\Gamma$  by  $N$ . Then the quotient group  $G/N$  acts on the quotient set  $\Gamma/N$ . In particular, for  $\sigma \in G$ , the length of any  $\sigma$ -orbit on the quotient set  $\Gamma/N$  is a divisor of the order of  $\sigma$  in the quotient group  $G/N$ .

### 3 Three kinds of duadic constacyclic codes

We keep notations introduced in Section 2. In this section we define three kinds of duadic constacyclic codes and study their properties. We begin with a class of isometries between constacyclic codes, which is a generalization of the multipliers for cyclic codes (cf. [15, §4.3, eq.(4.4)]).

**Lemma 3.1.** *Let  $t$  be an integer coprime to  $nr$  and  $\bar{t}$  be a positive integer such that  $t\bar{t} = 1 \pmod{nr}$ . Then the following map (where  $R_{n,\lambda^t} = F_q[X]/\langle X^n - \lambda^t \rangle$ , cf. Eq. (2.1))*

$$\varphi_t : R_{n,\lambda} \longrightarrow R_{n,\lambda^t}, \quad \sum_{i=0}^{n-1} a_i X^i \longmapsto \sum_{i=0}^{n-1} a_i X^{\bar{t}i} \pmod{X^n - \lambda^t},$$

is an algebra isomorphism and preserves the Hamming weights of words, i.e.,  $w(\varphi_t(a(X))) = w(a(X))$  for any  $a(X) \in R_{n,\lambda}$ .

**Proof.** For the polynomial algebra  $F_q[X]$  it is obvious that the following map

$$F_q[X] \longrightarrow F_q[X], \quad \sum_i a_i X^i \longmapsto \sum_i a_i X^{\bar{t}i},$$

is an algebra homomorphism. Hence it induces an algebra homomorphism:

$$\begin{aligned} \hat{\varphi}_t : F_q[X] &\longrightarrow F_q[X]/\langle X^n - \lambda^t \rangle, \\ \sum_i a_i X^i &\longmapsto \sum_i a_i X^{\bar{t}i} \pmod{X^n - \lambda^t}. \end{aligned}$$

In the algebra  $R_{n,\lambda^t} = F_q[X]/\langle X^n - \lambda^t \rangle$  we have the following computation:

$$\hat{\varphi}_t(X^n - \lambda) = X^{n\bar{t}} - \lambda = (\lambda^t)^{\bar{t}} - \lambda = 0 \pmod{X^n - \lambda^t}.$$

The algebra homomorphism  $\hat{\varphi}_t$  induces an algebra homomorphism as follows.

$$\begin{aligned} \varphi_t : F_q[X]/\langle X^n - \lambda \rangle &\longrightarrow F_q[X]/\langle X^n - \lambda^t \rangle, \\ \sum_{i=0}^{n-1} a_i X^i &\longmapsto \sum_{i=0}^{n-1} a_i X^{\bar{t}i} \pmod{X^n - \lambda^t}. \end{aligned}$$

That is,  $\varphi_t(a(X)) = a(X^{\bar{t}}) \pmod{X^n - \lambda^t}$  for  $a(X) \in R_{n,\lambda}$ . Since  $\lambda^r = 1$ , the  $\lambda^t$  and the algebra homomorphism  $\varphi_t$  are uniquely determined by  $t$  (independent of the choice of  $\bar{t}$ ) up to modulo  $nr$ .

For any  $i$  with  $0 \leq i < n$ , there are a unique  $t_i$  with  $0 \leq t_i < n$  and a unique  $q_i$  such that  $\bar{t}i = nq_i + t_i$ . Thus, in  $R_{n,\lambda^t}$  we have

$$\varphi_t\left(\sum_{i=0}^{n-1} a_i X^i\right) = \sum_{i=0}^{n-1} a_i X^{\bar{t}i} = \sum_{i=0}^{n-1} a_i \lambda^{tq_i} X^{t_i}. \quad (3.1)$$

The map  $i \mapsto t_i$  is a permutation of the index set  $\{0, 1, \dots, n-1\}$  and all  $\lambda^{tq_i} \neq 0$ . Let  $M_t$  be the monomial matrix which is the product of the diagonal matrix with diagonal elements  $\lambda^{tq_i}$  for  $i = 0, 1, \dots, n-1$  and the permutation matrix corresponding to the permutation  $i \mapsto t_i$  for  $i = 0, 1, \dots, n-1$ . Then Eq. (3.1) implies that:

- When  $\sum_{i=0}^{n-1} a_i X^i$  is viewed as the word  $(a_0, a_1, \dots, a_{n-1})$ , the map  $\varphi_t$  corresponds to the monomial equivalence on  $F_q^n$  by multiplying the monomial matrix  $M_t$ .

In particular,  $\varphi_t$  is an algebra isomorphism, and  $w(\varphi_t(a(X))) = w(a(X))$  for any  $a(X) \in R_{n,\lambda}$ .  $\square$

We call  $\varphi_t$  defined in the above lemma an *isometry* from  $R_{n,\lambda}$  to  $R_{n,\lambda^t}$ . Note that more general isometries were introduced in [8], but Lemma 3.1 contains more precise information for our later citations.

For example, if  $t = -1$ , then we can take  $\bar{t} = nr - 1$ . Noting that  $\lambda X^n \equiv 1 \pmod{X^n - \lambda^{-1}}$ , for  $a(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in R_{n,\lambda}$  we have

$$\varphi_{-1}(a(X)) \equiv \lambda X^n \sum_{i=0}^{n-1} a_i X^{i(nr-1)} \equiv \sum_{i=0}^{n-1} \lambda a_i X^{nri} X^{n-i} \pmod{X^n - \lambda^{-1}}.$$

Since  $X^{nr} \equiv 1 \pmod{X^n - \lambda^{-1}}$ , we get

$$\varphi_{-1}(a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) = a_0 + \lambda a_{n-1}X + \cdots + \lambda a_1X^{n-1}. \quad (3.2)$$

Next, we refine the set  $P_{n,\lambda^t}$  in (2.3) and the group  $G_{n,r}$  in (2.4) for any  $t \in \mathbb{Z}_{nr}^*$ . The decomposition  $n = n_r n'_r$  introduced in the following remark will be used throughout the paper.

**Remark 3.2.** Let  $n'_r$  be the maximal divisor of the integer  $n$  which is coprime to  $r$ . Hence  $n = n_r n'_r$  such that  $n'_r$  is coprime to  $r$ , and  $p|r$  for any prime divisor  $p|n_r$ . Let  $t \in \mathbb{Z}_{nr}^*$  as before. By the Chinese Remainder Theorem (cf. [7, eq.(IV.3), eq.(IV.4)] for details),

$$\begin{aligned} P_{n,\lambda^t} &= t + r\mathbb{Z}_{nr} \stackrel{\text{CRT}}{\equiv} (t + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}, \\ G_{n,r} &= \mathbb{Z}_{nr}^* \cap (1 + r\mathbb{Z}_{nr}) \stackrel{\text{CRT}}{\equiv} (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}^*, \end{aligned} \quad (3.3)$$

where  $\stackrel{\text{CRT}}{\equiv}$  stands for the equivalence by the Chinese Remainder Theorem, and  $1 + r\mathbb{Z}_{n_r r}$  is a subgroup of  $\mathbb{Z}_{n_r r}^*$  with order  $|1 + r\mathbb{Z}_{n_r r}| = n_r$  (see Lemma 4.3 below for more details). The group  $G_{n,r}$  acts on  $P_{n,\lambda^t}$  with  $1 + r\mathbb{Z}_{n_r r}$  and  $\mathbb{Z}_{n'_r}^*$  respectively acting on  $t + r\mathbb{Z}_{n_r r}$  and  $\mathbb{Z}_{n'_r}$  respectively.

There is a distinguished subset  $P_{n,\lambda^t}^{(0)}$  of  $P_{n,\lambda^t}$  as follows:

$$P_{n,\lambda^t}^{(0)} \stackrel{\text{CRT}}{\equiv} (t + r\mathbb{Z}_{n_r r}) \times \{0\} \subseteq (t + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}; \quad (3.4)$$

that is,  $P_{n,\lambda^t}^{(0)}$  consists of the elements of  $P_{n,\lambda^t}$  which are divisible by  $n'_r$ . It is easy to see that  $P_{n,\lambda^t}^{(0)}$  is  $\mu_s$ -invariant for any  $s \in G_{n,r}$ . In particular,  $P_{n,\lambda^t}^{(0)}$  is a union of some  $q$ -cosets. Let  $\bar{n}'_r$  be an integer such that  $n'_r \bar{n}'_r \equiv 1 \pmod{r}$ . For  $i \in P_{n,\lambda^t}^{(0)}$ , we can write  $i = i' n'_r$ ; since  $i' n'_r \equiv t \pmod{r}$ , we see that  $i' \equiv t \bar{n}'_r \pmod{r}$ . Thus

$$f_{P_{n,\lambda^t}^{(0)}}(X) = \prod_{i \in P_{n,\lambda^t}^{(0)}} (X - \theta^i) = X^{n_r} - \lambda^{t \bar{n}'_r}.$$

Generalizing the notations for negacyclic codes in [4], we make the following definition for general constacyclic codes.

**Definition 3.3.** Let  $t \in \mathbb{Z}_{nr}^*$  and  $s \in G_{n,r}$  (then  $\varphi_s$  is an isometry of  $R_{n,\lambda^t}$  to itself). By  $C_{n,\lambda^t}^{(0)} = C_{P_{n,\lambda^t}^{(0)}}^{(0)}$  we denote the  $\lambda^t$ -constacyclic code with check set  $P_{n,\lambda^t}^{(0)}$ , i.e.,  $X^{n_r} - \lambda^{t \bar{n}'_r}$  is a check polynomial of  $C_{n,\lambda^t}^{(0)}$ , where  $\bar{n}'_r$  is an integer such that  $n'_r \bar{n}'_r \equiv 1 \pmod{r}$ . Let  $C \subseteq R_{n,\lambda^t}$  be a  $\lambda^t$ -constacyclic code.

- (i) If  $R_{n,\lambda^t} = C \oplus \varphi_s(C)$ , i.e.,  $R_{n,\lambda^t} = C + \varphi_s(C)$  and  $C \cap \varphi_s(C) = 0$ , then we say that  $C$  and  $\varphi_s(C)$  are a pair of *Type-I duadic  $\lambda^t$ -constacyclic codes*.
- (ii) If  $R_{n,\lambda^t} = C_{n,\lambda^t}^{(0)} \oplus C \oplus \varphi_s(C)$ , then we say that  $C$  and  $\varphi_s(C)$  are a pair of *even-like duadic  $\lambda^t$ -constacyclic codes*, which are also named a pair of *Type-II duadic  $\lambda^t$ -constacyclic codes*.
- (iii) If  $R_{n,\lambda^t} = C + \varphi_s(C)$  and  $C \cap \varphi_s(C) = C_{n,\lambda^t}^{(0)}$ , then we say that  $C$  and  $\varphi_s(C)$  are a pair of *odd-like duadic  $\lambda^t$ -constacyclic codes*.

Note that, if  $C$  and  $\varphi_s(C)$  are a pair of even-like (i.e., Type-II) duadic  $\lambda^t$ -constacyclic codes, i.e.,  $R_{n,\lambda^t} = C_{n,\lambda^t}^{(0)} \oplus C \oplus \varphi_s(C)$ , then  $\varphi_s^2(C) = C$  because  $\varphi_s^2(C_{n,\lambda^t}^{(0)}) = C_{n,\lambda^t}^{(0)}$ . It is the same for Type-I duadic  $\lambda^t$ -constacyclic codes and odd-like duadic  $\lambda^t$ -constacyclic codes.

If  $C$  and  $\varphi_s(C)$  are a pair of even-like  $\lambda^t$ -constacyclic codes, then from the direct sum  $R_{n,\lambda^t} = C_{n,\lambda^t}^{(0)} \oplus C \oplus \varphi_s(C)$  it is easy to see that  $C' = C_{n,\lambda^t}^{(0)} \oplus C$  and  $\varphi_s(C') = C_{n,\lambda^t}^{(0)} \oplus \varphi_s(C)$  are a pair of odd-like duadic  $\lambda^t$ -constacyclic codes.

Conversely, assume that  $C'$  and  $\varphi_s(C')$  are a pair of odd-like duadic  $\lambda^t$ -constacyclic codes. Since  $R_{n,\lambda^t}$  is a semisimple algebra (i.e.  $X^n - \lambda^t$  has no multiple roots), there is a unique ideal  $C$  such that  $C' = C_{n,\lambda^t}^{(0)} \oplus C$ , hence  $\varphi_s(C') = C_{n,\lambda^t}^{(0)} \oplus \varphi_s(C)$ . Then  $C$  and  $\varphi_s(C)$  are a pair of even-like duadic  $\lambda^t$ -constacyclic codes.

We show an example. Let  $q = 5$ ,  $n = 6$  and  $\lambda = 2 \in F_5^*$  (so  $r = 4$ ). Then  $R_{n,\lambda} = F_5[X]/\langle X^6 - 2 \rangle$ ,  $nr = 24$ ,  $n_r = 2$ ,  $n'_r = 3$ ,  $P_{n,\lambda} = \{1, 5, 9, 13, 17, 21\}$ ,  $P_{n,\lambda}^{(0)} = \{9, 21\}$ . Take  $s = \bar{s} = 13$ , then  $s\bar{s} \equiv 1 \pmod{24}$ . It is easy to check that

$$X^6 - 2 = (X^2 - 3)(X^2 + X + 2)(X^2 - X + 2),$$

and  $f_{P_{n,\lambda}^{(0)}}(X) = X^2 - 3$ . Let  $C \subseteq R_{n,\lambda}$  be the  $\lambda$ -constacyclic code with check polynomial  $X^2 + X + 2$ . Since  $\varphi_{13}(X^2 + X + 2) = X^2 - X + 2$ , we have the direct sum  $R_{n,\lambda} = C_{n,\lambda}^{(0)} \oplus C \oplus \varphi_{13}(C)$ . Thus,  $C$  and  $\varphi_{13}(C)$  are a pair of even-like (Type-II) duadic  $\lambda$ -constacyclic codes. On the other hand,  $C_{n,\lambda}^{(0)} \oplus C$  and  $C_{n,\lambda}^{(0)} \oplus \varphi_{13}(C)$  are a pair of odd-like duadic  $\lambda$ -constacyclic codes. In fact, this example is a specific instance of Proposition 5.1 below.

The following lemma shows that the isometry  $\varphi_t : R_{n,\lambda} \rightarrow R_{n,\lambda^t}$  is related closely to the bijection  $\mu_t : P_{n,\lambda} \rightarrow P_{n,\lambda^t}$ .

**Lemma 3.4.** *Let  $t \in \mathbb{Z}_{nr}^*$ . If  $C_P \subseteq R_{n,\lambda}$  is a  $\lambda$ -constacyclic code with check set  $P \subseteq P_{n,\lambda}$ , then*

$$\varphi_t(C_P) = C_{tP} \subseteq R_{n,\lambda^t}$$

*is a  $\lambda^t$ -constacyclic code, i.e.,  $f_{tP}(X) = \prod_{Q \in tP/\mu_q} f_Q(X)$  is a check polynomial of the  $\lambda^t$ -constacyclic code  $\varphi_t(C_P)$ .*



**Proof.** Let  $c(X) \in C_P$ . By Remark 2.1,  $c(\theta^i) = 0$  for all  $i \in P_{n,\lambda} \setminus P$ . By the definition of  $\varphi_t$  in Lemma 3.1,  $\varphi_t(c(X)) = c(X^{\bar{t}}) + b(X)(X^n - \lambda^t)$  for some  $b(X) \in F_q[X]$ , where  $t, \bar{t} \in \mathbb{Z}_{nr}^*$  satisfying that  $t\bar{t} = 1 \pmod{nr}$ . Hence

$$\varphi_t(c(\theta^i)) = c(\theta^{\bar{t}i}) + b(\theta^i)(\theta^{in} - \lambda^t) = 0, \quad \forall i \in P_{n,\lambda^t} \setminus tP.$$

So  $\varphi_t(c(X)) \in C_{tP}$ , see Remark 2.1. Since  $\varphi_t$  is an algebra isomorphism,

$$\dim(\varphi_t(C_P)) = \dim(C_P) = |P| = |tP| = \dim(C_{tP}),$$

where  $|P|$  denotes the cardinality of the set  $P$ . Thus  $\varphi_t(C_P) = C_{tP}$ .  $\square$

By replacing a permutation equivalence  $\Phi$  defined in [5] with the isometry  $\varphi_{-1}$  defined in Lemma 3.1, we modify [5, Th.4] as follows:

**Lemma 3.5.** *Let  $C \subseteq R_{n,\lambda}$  be a  $\lambda$ -constacyclic code. Set*

$$\text{Ann}(C) = \{a(X) \in R_{n,\lambda} \mid a(X)c(X) = 0 \text{ in } R_{n,\lambda}, \forall c(X) \in C\},$$

*which is also a  $\lambda$ -constacyclic code. Then*

$$C^\perp = \varphi_{-1}(\text{Ann}(C)) \subseteq R_{n,\lambda^{-1}}$$

*is a  $\lambda^{-1}$ -constacyclic code.*

**Proof.** Let  $a(X) = \sum_{i=0}^{n-1} a_i X^i \in \text{Ann}(C)$ . In  $R_{n,\lambda}$ , since  $XX^{n-1} = \lambda$  is invertible,  $X$  is invertible. For  $c(X) \in C$ , there is a  $b(X) = \sum_{i=0}^{n-1} b_i X^i \in C$  such that  $Xb(X) = c(X)$ . In  $R_{n,\lambda}$ , since  $c(X)a(X) = 0$ ,  $b(X)a(X) = 0$ . Considering the coefficient of  $X^{n-1}$ , we get

$$b_0 a_{n-1} + b_1 a_{n-2} + \cdots + b_{n-1} a_0 = 0.$$

In  $R_{n,\lambda^{-1}}$ , by Eq. (3.2),

$$\lambda^{-1} \varphi_{-1}(a(X)) = \lambda^{-1} a_0 + a_{n-1} X + \cdots + a_1 X^{n-1}.$$

Noting that, in  $R_{n,\lambda}$ ,  $Xb(X)$  is corresponding to the word  $(\lambda b_{n-1}, b_0, \dots, b_{n-2})$ , we obtain that

$$\lambda^{-1} \langle c(X), \varphi_{-1}(a(X)) \rangle = \langle Xb(X), \lambda^{-1} \varphi_{-1}(a(X)) \rangle = 0.$$

In conclusion,  $\varphi_{-1}(a(X)) \in C^\perp$ . Thus  $\varphi_{-1}(\text{Ann}(C)) \subseteq C^\perp$ . Since  $\dim C^\perp = n - \dim C = \dim \text{Ann}(C)$ , we get  $C^\perp = \varphi_{-1}(\text{Ann}(C))$ .  $\square$

Since  $R_{n,\lambda}$  is a semisimple algebra, for any  $\mu_q$ -invariant subset  $P \subseteq P_{n,\lambda}$ , it is easy (cf. Eq. (2.6)) to see that

$$\text{Ann}(C_P) = C_{\overline{P}}, \quad \text{where } \overline{P} = P_{n,\lambda} \setminus P. \quad (3.5)$$

Combining it with Lemma 3.5 and Lemma 3.4, we have an immediate corollary.

**Corollary 3.6.** *With notations in (3.5),  $C_P^\perp = C_{-\overline{P}} = C_{\overline{-P}}$ , where  $-P = (-1)P$  and  $\overline{-P} = P_{n,\lambda^{-1}} \setminus (-P)$ .*

**Theorem 3.7.** *Let  $C \subseteq R_{n,\lambda}$  be a  $\lambda$ -constacyclic code and  $s \in G_{n,r}$ . Then  $C$  and  $\varphi_s(C)$  are a pair of even-like duadic  $\lambda$ -constacyclic codes if and only if  $C^\perp$  and  $\varphi_s(C)^\perp$  are a pair of odd-like duadic  $\lambda^{-1}$ -constacyclic codes.*

**Proof.** Let  $C = C_P$  with check set  $P \subseteq P_{n,\lambda}$ . Then  $\varphi_s(C) = C_{sP}$  with check set  $sP \subseteq P_{n,\lambda}$ . Assume that  $C$  and  $\varphi_s(C)$  are even-like duadic  $\lambda$ -constacyclic codes, i.e.,  $R_{n,\lambda} = C_{n,\lambda}^{(0)} + C_P + C_{sP}$ ,  $C_{n,\lambda}^{(0)} \cap (C_P + C_{sP}) = 0$  and  $C_P \cap C_{sP} = 0$ . By Eq. (2.7),  $P_{n,\lambda} = P_{n,\lambda}^{(0)} \cup P \cup sP$  and  $P_{n,\lambda}^{(0)}$ ,  $P$ ,  $sP$  are pairwise disjoint. Note that  $\mu_{-1}$  transforms  $P_{n,\lambda}$  to  $P_{n,\lambda^{-1}}$  bijectively and  $-P_{n,\lambda}^{(0)} = P_{n,\lambda^{-1}}^{(0)}$  obviously. We get that  $P_{n,\lambda^{-1}} = P_{n,\lambda^{-1}}^{(0)} \cup (-P) \cup (-sP)$  and  $P_{n,\lambda^{-1}}^{(0)}$ ,  $-P$ ,  $-sP$  are pairwise disjoint. So

$$\begin{aligned}\overline{-P} &= P_{n,\lambda^{-1}} \setminus (-P) = P_{n,\lambda^{-1}}^{(0)} \cup (-sP), \\ \overline{-sP} &= P_{n,\lambda^{-1}} \setminus (-sP) = P_{n,\lambda^{-1}}^{(0)} \cup (-P).\end{aligned}$$

In  $R_{n,\lambda^{-1}}$ , by Corollary 3.6 we have  $C_P^\perp = C_{\overline{-P}}$  and  $C_{sP}^\perp = C_{\overline{-sP}}$ . By Eq. (2.7), from the above equalities we obtain that

$$R_{n,\lambda^{-1}} = C_P^\perp + C_{sP}^\perp, \quad C_P^\perp \cap C_{sP}^\perp = C_{P_{n,\lambda^{-1}}^{(0)}} = C_{n,\lambda^{-1}}^{(0)}.$$

Thus,  $C_P^\perp$  and  $C_{sP}^\perp = \varphi_s(C_P)^\perp$  are odd-like duadic  $\lambda^{-1}$ -constacyclic codes.

Conversely, assume that  $C_P^\perp$  and  $C_{sP}^\perp$  are odd-like duadic  $\lambda^{-1}$ -constacyclic codes. It is easy to check that all the arguments in the above paragraph can be reversed. Thus we can backward step by step to reach the conclusion that  $C_P$  and  $\varphi_s(C_P)$  are even-like duadic  $\lambda$ -constacyclic codes.  $\square$

In the special case where  $r = 1$  (i.e., cyclic codes are considered) and  $s = -1$ , the result [15, Th. 6.4.2] is a consequence of the above theorem.

**Lemma 3.8.** *Let  $t \in \mathbb{Z}_{nr}^*$ , and  $C_P \subseteq R_{n,\lambda}$  be a  $\lambda$ -constacyclic code with check set  $P \subseteq P_{n,\lambda}$ . Then the following conditions are equivalent.*

- (i)  $\varphi_t(C_P) \subseteq C_P^\perp$  (in the case we call  $C$  a  $\varphi_t$ -isometrically orthogonal code).
- (ii)  $\varphi_{-t}(C) \subseteq R_{n,\lambda}$  and  $C_P \cap \varphi_{-t}(C_P) = 0$ .
- (iii)  $-t \in G_{n,r}$  and  $P \cap (-tP) = \emptyset$ .

**Proof.** (i)  $\Leftrightarrow$  (iii). By Lemma 3.4 and Corollary 3.6, (i) holds if and only if  $C_{tP} \subseteq C_{\overline{-P}}$  where  $\overline{-P} = P_{n,\lambda^{-1}} \setminus (-P)$ ; by Eq. (2.7), it is equivalent to that  $tP \subseteq \overline{-P} = -\overline{P}$  where  $\overline{P} = P_{n,\lambda} \setminus P$ ; i.e.,  $-tP \subseteq \overline{P}$ , (iii) holds.

(ii)  $\Leftrightarrow$  (iii). “ $\varphi_{-t}(C) \subseteq R_{n,\lambda}$ ” is obviously equivalent to “ $-t \in G_{n,r}$ ”. Note that  $\varphi_{-t}(C_P) = C_{-tP}$ . Then, by Eq. (2.7),  $C_P \cap \varphi_{-t}(C_P) = 0$  if and only if  $P \cap (-tP) = \emptyset$ .  $\square$

Taking  $t = 1$  in Lemma 3.8, we get a known consequence:

**Corollary 3.9.** *A  $\lambda$ -constacyclic code  $C_P \leq R_{n,\lambda}$  with check set  $P \subseteq P_{n,\lambda}$  is self-orthogonal if and only if  $\lambda = \pm 1$  and  $P \cap (-P) = \emptyset$ .*

Generalizing the self-orthogonality, we consider the iso-orthogonality.

**Definition 3.10.** Let  $C \subseteq R_{n,\lambda}$  be a  $\lambda$ -constacyclic code.

- (i) If there is an  $s \in G_{n,r}$  such that  $C$  is  $\varphi_{-s}$ -isometrically orthogonal (i.e., Lemma 3.8(i) for  $t = -s$  holds), then we say that  $C$  is *isometrically self-orthogonal*, or *iso-orthogonal* for short.
- (ii) If there is an  $s \in G_{n,r}$  such that both  $C$  and  $\varphi_s(C)$  are  $\varphi_{-s}$ -isometrically orthogonal (hence  $C \cap \varphi_s(C) = 0$ , see Lemma 3.8(ii)) and  $\varphi_s^2(C) = C$ , then we say that  $C, \varphi_s(C)$  are an *iso-orthogonal pair* of  $\lambda$ -constacyclic codes.
- (iii) An iso-orthogonal pair  $C, \varphi_s(C)$  of  $\lambda$ -constacyclic codes is said to be *maximal* if for any iso-orthogonal pair  $C', \varphi_{s'}(C')$  of  $\lambda$ -constacyclic codes we have  $\dim C' \leq \dim C$ .

If  $C_P, \varphi_s(C_P)$  are Type-I duadic  $\lambda$ -constacyclic codes, i.e.,  $P_{n,\lambda} = P \cup (sP)$  is a partition, then  $C_P, \varphi_s(C_P)$  are of course a maximal iso-orthogonal pair of  $\lambda$ -constacyclic codes. In fact, in that case both  $C_P$  and  $\varphi_s(C_P)$  are *iso-dual  $\lambda$ -constacyclic codes*, see [5]. Otherwise, if the Type-I duadic constacyclic codes do not exist, then we show that any pair of even-like duadic constacyclic codes is a maximal iso-orthogonal pair of constacyclic codes provided it does exist.

**Lemma 3.11.** *Type-I duadic  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  exist if and only if the order of the quotient group  $(1 + r\mathbb{Z}_{n,r})/\langle q \rangle_{\mathbb{Z}_{n,r}^*}^*$  is even, where  $\langle q \rangle_{\mathbb{Z}_{n,r}^*}^*$  denotes the subgroup of  $\mathbb{Z}_{n,r}^*$  generated by  $q$ .*

**Proof.** Note that  $q \in 1 + r\mathbb{Z}_{n,r}$  hence  $\langle q \rangle_{\mathbb{Z}_{n,r}^*}^* \subseteq 1 + r\mathbb{Z}_{n,r}$ . This lemma has been included in [7, Th.4] where more complicated results are proved. For convenience, we sketch a quick proof of the lemma. If  $(1 + r\mathbb{Z}_{n,r})/\langle q \rangle_{\mathbb{Z}_{n,r}^*}^*$  is of even order, we take  $s_0 \in 1 + r\mathbb{Z}_{n,r}$  such that in the quotient group the element  $s_0$  has order 2; and take  $s \in G_{n,r}$  such that  $s \stackrel{\text{CRT}}{=} (s_0, 1) \in (1 + r\mathbb{Z}_{n,r}) \times \mathbb{Z}_{n_r'}^*$ , cf. Eq. (3.3). By Remark 2.2(iii) and (iv), it is easy to see that any  $s$ -orbit on  $P_{n,\lambda}/\mu_q$  has length 2. By Remark 2.2(ii), there is a  $\mu_q$ -invariant subset  $P \subseteq P_{n,\lambda}$  such that  $P_{n,\lambda} = P \cup sP$  is a partition. Hence  $C_P$  and  $C_{sP}$  are a pair of Type-I duadic  $\lambda$ -constacyclic codes.

Conversely, if  $C_P$  and  $C_{sP}$  are a pair of Type-I duadic  $\lambda$ -constacyclic codes, by Remark 2.2(ii), the length of any  $s$ -orbit on  $P_{n,\lambda}^{(0)}/\mu_q$  is even; so in the quotient group  $(1 + r\mathbb{Z}_{n,r})/\langle q \rangle_{\mathbb{Z}_{n,r}^*}^*$  the order of the element  $s$  is even (cf. Remark 2.2(i)). Hence the order of the group  $(1 + r\mathbb{Z}_{n,r})/\langle q \rangle_{\mathbb{Z}_{n,r}^*}^*$  is even.  $\square$

**Theorem 3.12.** *Assume that Type-I duadic  $\lambda$ -constacyclic codes of length  $n$  do not exist but Type-II (i.e., even-like) duadic  $\lambda$ -constacyclic codes of length  $n$  exist. Then any pair  $C_P, \varphi_s(C_P)$  of Type-II duadic  $\lambda$ -constacyclic codes of length  $n$  is a maximal iso-orthogonal pair of  $\lambda$ -constacyclic codes.*

**Proof.** By Lemma 3.11 and the assumption of the theorem, the order of the quotient group  $(1 + r\mathbb{Z}_{n,r})/\langle q \rangle_{\mathbb{Z}_{n,r}^*}$  is odd. Then, by Remark 2.2(iv), for any  $s' \in G_{n,r}$ , the length of any  $s'$ -orbit on the quotient set  $P_{n,\lambda}^{(0)}/\mu_q$  is odd.

Now we prove the theorem by contradiction. Suppose that  $C_{P'}$  and  $\varphi_{s'}(C_{P'})$  are an iso-orthogonal pair of  $\lambda$ -constacyclic codes such that

$$\dim C_{P'} > \dim C_P = |P| = \frac{n - n_r}{2}.$$

Set  $P'' = P' \cap P_{n,\lambda}^{(0)} \subseteq P_{n,\lambda}^{(0)}$ . Since  $s'P_{n,\lambda}^{(0)} = P_{n,\lambda}^{(0)}$ ,  $s'P'' = s'P' \cap P_{n,\lambda}^{(0)} \subseteq P_{n,\lambda}^{(0)}$ . Because  $P' \cap (s'P') = \emptyset$ , we have  $P'' \cap s'P'' = \emptyset$  and

$$|P' \cup (s'P')| = |P'| + |s'P'| = 2|P'| = 2 \dim C_{P'} > n - n_r = |P_{n,\lambda} \setminus P_{n,\lambda}^{(0)}|.$$

Thus,  $P''$  and  $s'P''$  are non-empty subsets of  $P_{n,\lambda}^{(0)}$  such that  $P'' \cap s'P'' = \emptyset$  and  $s'^2P'' = P''$ . Note that both  $P''$  and  $s'P''$  are  $\mu_q$ -invariant. The permutation  $\mu_{s'}$  gives a bijection from the quotient set  $P''/\mu_q$  to the quotient set  $s'P''/\mu_q$ . Thus, the length of any  $s'$ -orbit on the quotient set  $(P'' \cup s'P'')/\mu_q$  is even. This is a contradiction.  $\square$

## 4 Existence of Type-II duadic constacyclic codes

We keep notations introduced in Section 2, and describe the decomposition  $n = n_r n'_r$  in Remark 3.2 more precisely. Assume that  $r_1, \dots, r_h, r'_1, \dots, r'_{h'}$ ,  $p_1, \dots, p_\ell$  are distinct primes such that

$$\begin{aligned} r &= r_1^{e_1} \cdots r_h^{e_h} r'_1{}^{e'_1} \cdots r'_{h'}{}^{e'_{h'}}; & h, h' \geq 0; & \text{all } e_i, e'_i \text{ are positive;} \\ n &= r_1^{u_1} \cdots r_h^{u_h} p_1^{v_1} \cdots p_\ell^{v_\ell}, & \ell \geq 1, & \text{all } u_i, v_i \text{ are positive.} \end{aligned} \quad (4.1)$$

Then  $n = n_r n'_r$  where

$$n_r = r_1^{u_1} \cdots r_h^{u_h}, \quad n'_r = p_1^{v_1} \cdots p_\ell^{v_\ell}. \quad (4.2)$$

In this section we consider Eq. (3.3) and Eq. (3.4) only for  $t = 1$ , as restated below.

$$\begin{aligned} P_{n,\lambda} &= 1 + r\mathbb{Z}_{nr} \stackrel{\text{CRT}}{\cong} (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}, \\ G_{n,r} &= \mathbb{Z}_{nr}^* \cap (1 + r\mathbb{Z}_{nr}) \stackrel{\text{CRT}}{\cong} (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}^*, \end{aligned} \quad (4.3)$$

$$P_{n,\lambda}^{(0)} \stackrel{\text{CRT}}{\cong} (1 + r\mathbb{Z}_{n_r r}) \times \{0\} \subseteq (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{n'_r}. \quad (4.4)$$

The main result of this section is as follows.

**Theorem 4.1.** *Type-II duadic  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  exist if and only if one of the following two holds.*

- (i)  $n_r$  is even (equivalently, both  $n$  and  $r$  are even).
- (ii)  $n$  is odd and  $q$  is a square of an element in  $\mathbb{Z}_{n'_r}$ .

We will prove it in two cases. Case 1:  $n_r$  is even, see Theorem 4.4 below. Case 2:  $n_r$  is odd, see Theorem 4.6 below.

Corresponding to Definition 3.3, we have the following definition.

**Definition 4.2.** Let notations be as in Eq. (4.3) and Eq. (4.4). Let  $P \subseteq P_{n,\lambda}$  and  $s \in G_{n,r}$ .

- (i) If  $P_{n,\lambda} = P \cup (sP)$  is a partition, then  $P, sP$  are called a *Type-I duadic splitting* of  $P_{n,\lambda}$  given by  $\mu_s$  (and  $C_P, C_{sP}$  are a pair of Type-I duadic  $\lambda$ -constacyclic codes).
- (ii) If  $P_{n,\lambda} = P_{n,\lambda}^{(0)} \cup P \cup (sP)$  is a partition, then  $P, sP$  are called a *Type-II duadic splitting* of  $P_{n,\lambda}$  given by  $\mu_s$  (and  $C_P, C_{sP}$  are a pair of Type-II (i.e., even-like) duadic  $\lambda$ -constacyclic codes in Definition 3.3(ii)).

Similarly as in Definition 3.3, it is easy to check that with above definitions we have  $s^2P = P$ .

We need more precise information on the subgroup  $1 + r\mathbb{Z}_{n,r}$  of  $\mathbb{Z}_{n,r}^*$ .

**Lemma 4.3.** *With notations in (4.2)-(4.4), the following hold.*

- (i)  $1 + r\mathbb{Z}_{n,r} \stackrel{\text{CRT}}{=} (1 + r_1^{e_1} \mathbb{Z}_{r_1^{e_1+u_1}}) \times \cdots \times (1 + r_h^{e_h} \mathbb{Z}_{r_h^{e_h+u_h}})$ , and the order of the direct factor  $|(1 + r_i^{e_i} \mathbb{Z}_{r_i^{e_i+u_i}})| = r_i^{u_i}$  for  $i = 1, \dots, h$ . Hence, the cardinality  $|1 + r\mathbb{Z}_{n,r}| = |P_{n,\lambda}^{(0)}| = n_r$ .
- (ii) The group  $1 + r\mathbb{Z}_{n,r}$  has even order if and only if both  $n$  and  $r$  are even. If this is the case, assuming that  $r_1 = 2$ ,  $e = e_1 \geq 1$  and  $u = u_1 \geq 1$ , we have

$$1 + r\mathbb{Z}_{n,r} \stackrel{\text{CRT}}{=} (1 + 2^e \mathbb{Z}_{2^{e+u}}) \times (1 + r_2^{e_2} \mathbb{Z}_{r_2^{e_2+u_2}}) \times \cdots \times (1 + r_h^{e_h} \mathbb{Z}_{r_h^{e_h+u_h}})$$

with  $1 + 2^e \mathbb{Z}_{2^{e+u}}$  being the Sylow 2-subgroup of  $1 + r\mathbb{Z}_{n,r}$ .

- (iii) Type-I duadic splittings of  $P_{n,\lambda}$  exist if and only if both  $n$  and  $r$  are even and  $\langle q \rangle_{\mathbb{Z}_{2^{e+u}}^*} \not\subseteq 1 + 2^e \mathbb{Z}_{2^{e+u}}$ , where  $\langle q \rangle_{\mathbb{Z}_{2^{e+u}}^*}$  denotes the subgroup of  $\mathbb{Z}_{2^{e+u}}^*$  generated by  $q$ .

**Proof.** (i). With the notation in (4.1), by the Chinese Remainder Theorem we have (cf. [7, eq.(IV.3)] for more details):

$$\begin{aligned} 1 + r\mathbb{Z}_{n,r} &\stackrel{\text{CRT}}{=} (1 + r_1^{e_1} \mathbb{Z}_{r_1^{e_1+u_1}}) \times \cdots \times (1 + r_h^{e_h} \mathbb{Z}_{r_h^{e_h+u_h}}) \\ &\quad \times (1 + r_1^{e'_1} \mathbb{Z}_{r_1^{e'_1}}) \times \cdots \times (1 + r_{h'}^{e_{h'}} \mathbb{Z}_{r_{h'}^{e_{h'}}}). \end{aligned}$$

But  $1 + r_i^{e'_i} \mathbb{Z}_{r_i^{e'_i}} = \{1\}$  for  $i = 1, \dots, h'$ , and  $|(1 + r_i^{e_i} \mathbb{Z}_{r_i^{e_i+u_i}})| = r_i^{u_i}$  for  $i = 1, \dots, h$ . So (i) holds.

(ii) follows from (i).

(iii). By Lemma 3.11, Type-I duadic splittings of  $P_{n,\lambda}$  exist if and only if  $(1 + r\mathbb{Z}_{n_r r})/\langle q \rangle_{\mathbb{Z}_{n_r r}^*}$  is a group of even order; by (ii), this happens if and only if the quotient of the Sylow 2-subgroup  $(1 + 2^e \mathbb{Z}_{2^{e+u}})/\langle q \rangle_{\mathbb{Z}_{2^{e+u}}^*}$  is non-trivial, which happens if and only if (iii) holds.  $\square$

**Theorem 4.4.** *If both  $n$  and  $r$  are even, then the Type-II duadic  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  exist.*

**Proof.** Let notations be as in (4.2)-(4.4). Since both  $n$  and  $r$  are even, we can assume, as in Lemma 4.3(ii), that  $r_1 = 2$ ,  $e = e_1 \geq 1$  and  $u = u_1 \geq 1$ . If  $P \cup sP$  is a Type-I splitting of  $P_{n,\lambda}$  given by  $\mu_s$ , then  $P' = P \setminus (P_{n,\lambda}^{(0)} \cap P)$  is non-empty and it is easy to check that  $P' \cup sP'$  is a Type-II splitting of  $P_{n,\lambda}$  given by  $\mu_s$ . So we can further assume that Type-I duadic  $\lambda$ -constacyclic codes of length  $n$  do not exist. Hence, by Lemma 4.3(iii),  $q$  generates the multiplicative group  $1 + 2^e \mathbb{Z}_{2^{e+u}}$ , i.e.,  $\text{ord}_{\mathbb{Z}_{2^{e+u}}^*}(q) = 2^u$ .

To prove the existence of Type-II duadic  $\lambda$ -constacyclic codes of length  $n$ , by Remark 2.2 (i), (ii) and (iv), it is enough to show that there is an integer  $s \in G_{n,r}$  such that  $\text{ord}_{\mathbb{Z}_{n_r}^*}(s) = 2^f$  with  $f \geq 1$  and

$$sQ \neq Q, \quad \text{for any } q\text{-coset } Q \text{ on } P_{n,\lambda} \setminus P_{n,\lambda}^{(0)}. \quad (4.5)$$

By Lemma 4.3(ii), we write  $1 + r\mathbb{Z}_{n_r r} = (1 + 2^e \mathbb{Z}_{2^{e+u}}) \times L$  with  $L$  being a group of odd order. By Eq. (4.2), we refine Eq. (4.3) as follows:

$$\begin{aligned} P_{n,\lambda} &\stackrel{\text{CRT}}{=} (1 + 2^e \mathbb{Z}_{2^{e+u}}) \times L \times \mathbb{Z}_{p_1^{v_1}} \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}, \\ G_{n,r} &\stackrel{\text{CRT}}{=} (1 + 2^e \mathbb{Z}_{2^{e+u}}) \times L \times \mathbb{Z}_{p_1^{v_1}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}^*. \end{aligned}$$

Let  $1 \leq i \leq \ell$ . Then  $p_i$  is an odd prime and  $\mathbb{Z}_{p_i^{v_i}}^*$  is a cyclic group of order  $p_i^{v_i-1}(p_i - 1)$ . Since  $p_i - 1$  is coprime to  $p_i^{v_i-1}$ , there is a unique subgroup  $H_i$  of  $\mathbb{Z}_{p_i^{v_i}}^*$  such that

$$\mathbb{Z}_{p_i^{v_i}}^* = (1 + p_i \mathbb{Z}_{p_i^{v_i}}) \times H_i \quad (4.6)$$

and the natural homomorphism  $\mathbb{Z}_{p_i^{v_i}}^* \rightarrow \mathbb{Z}_{p_i}^*$  induces an isomorphism  $H_i \cong \mathbb{Z}_{p_i}^*$ . Note that  $2 \mid (p_i - 1) = |\mathbb{Z}_{p_i}^*|$ . We choose an integer  $s_i \in \mathbb{Z}_{p_i^{v_i}}^*$  for different cases.

Case 1: If  $\text{ord}_{\mathbb{Z}_{p_i^{v_i}}^*}(q)$  is odd, we take  $s_i \in H_i$  such that  $\text{ord}_{H_i}(s_i) = 2^{f_i}$  with  $f_i = 1$ ;

Case 2: if  $\text{ord}_{\mathbb{Z}_{p_i^{v_i}}^*}(q)$  is even, then there is an odd integer  $d_i$  such that the order  $\text{ord}_{\mathbb{Z}_{p_i^{v_i}}^*}(q^{d_i}) = 2^{f_i}$  with  $f_i \geq 1$  (hence  $q^{d_i} \in H_i$ ); in that case, we take  $s_i = q^{d_i}$ .

Let

$$s = (1, 1, s_1, \dots, s_\ell) \in (1 + 2^e \mathbb{Z}_{2^{e+u}}) \times L \times \mathbb{Z}_{p_1^{v_1}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}^*.$$

Then  $\text{ord}_{\mathbb{Z}_{nr}^*}(s) = 2^f$  where  $f = \max\{f_1, \dots, f_\ell\} \geq 1$ .

Let  $Q$  be any  $q$ -coset on  $P_{n,\lambda}$  outside  $P_{n,\lambda}^{(0)}$ , i.e.,  $Q \subseteq P_{n,\lambda} \setminus P_{n,\lambda}^{(0)}$ . Take

$$(\alpha, \alpha', \alpha_1, \dots, \alpha_\ell) \in Q \text{ with } \alpha \in 1 + 2^e \mathbb{Z}_{2^{e+u}}, \alpha' \in L, \alpha_i \in \mathbb{Z}_{p_i^{v_i}} \text{ for } i=1, \dots, \ell.$$

Since  $q$  generates  $1 + 2^e \mathbb{Z}_{2^{e+u}}$ , we have  $q^t \alpha \equiv 1 \pmod{2^{e+u}}$  for some integer  $t$ . Set  $k' = q^t \alpha' \in L$  and  $k_i = q^t \alpha_i \in \mathbb{Z}_{p_i^{v_i}}$  for  $i = 1, \dots, \ell$ . Then

$$(1, k', k_1, \dots, k_\ell) = q^t(\alpha, \alpha', \alpha_1, \dots, \alpha_\ell) \in Q.$$

Now we prove Eq. (4.5) by contradiction. Suppose that  $sQ = Q$ . Because  $Q \cap P_{n,\lambda}^{(0)} = \emptyset$ , there is an integer  $m$  with  $1 \leq m \leq \ell$  such that  $k_m \not\equiv 0 \pmod{p_m^{v_m}}$ . Since  $sQ = Q$ ,

$$s(1, k', k_1, \dots, k_m, \dots, k_\ell) = (1, k', s_1 k_1, \dots, s_m k_m, \dots, s_\ell k_\ell) \in Q.$$

Thus, there is an integer  $j$  such that

$$q^j(1, k', k_1, \dots, k_m, \dots, k_\ell) = (1, k', s_1 k_1, \dots, s_m k_m, \dots, s_\ell k_\ell).$$

In particular,

$$q^j \equiv 1 \pmod{2^{e+u}} \quad \text{and} \quad q^j k_m \equiv s_m k_m \pmod{p_m^{v_m}}.$$

Since  $\text{ord}_{\mathbb{Z}_{2^{e+u}}^*}(q) = 2^u$ , from the first equality we have  $j \equiv 0 \pmod{2^u}$ ; in particular,  $j$  is even. Next, write  $k_m = p_m^{v'_m} k'_m$  with  $p_m \nmid k'_m$ , then  $0 \leq v'_m < v_m$  because  $k_m \not\equiv 0 \pmod{p_m^{v_m}}$ . The second equality becomes:

$$q^j p_m^{v'_m} k'_m \equiv s_m p_m^{v'_m} k'_m \pmod{p_m^{v_m}}.$$

Hence  $q^j \equiv s_m \pmod{p_m^{v_m - v'_m}}$ . Since  $v_m - v'_m \geq 1$ , we get

$$q^j \equiv s_m \pmod{p_m}. \tag{4.7}$$

In Case 1, in the group  $\mathbb{Z}_{p_m}^*$  the order of the element  $q^j$  is odd, but the order of  $s_m$  is 2; it is a contradiction to Eq. (4.7).

In Case 2, in the group  $\mathbb{Z}_{p_m}^*$  the order of the element  $q$  is even; but  $j$  is even and  $d_m$  is odd, hence

$$\nu_2(\text{ord}_{\mathbb{Z}_{p_m}^*}(q^j)) < \nu_2(\text{ord}_{\mathbb{Z}_{p_m}^*}(q)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_m}^*}(q^{d_m})),$$

where  $\nu_2(t)$  denotes the 2-adic valuation of the integer  $t$ , i.e.  $2^{\nu_2(t)}$  is the maximal power of 2 dividing  $t$ . In particular,  $q^j \not\equiv q^{d_m} \pmod{p_m}$ , which contradicts Eq. (4.7), as we have chosen  $s_m = q^{d_m}$  in this case.

The contradictions finish the proof of the theorem.  $\square$

Taking  $r = 2$ , from Theorem 4.4 we get the following immediate consequence which has been proved in [4].

**Corollary 4.5** ([4]). *If  $n$  is even, then Type-II duadic negacyclic codes of length  $n$  over  $F_q$  exist.*

By  $\nu_2(t)$  we denote the 2-adic valuation of the integer  $t$  as before.

**Theorem 4.6.** *Let  $n = n_r n'_r$  and  $n'_r = p_1^{v_1} \cdots p_\ell^{v_\ell}$  as in (4.2). Assume that  $n_r$  is odd (equivalently,  $n$  or  $r$  is odd). Then the following three are equivalent to each other.*

- (i) *Type-II duadic  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  exist.*
- (ii) *For all  $i = 1, \dots, \ell$ ,  $p_i$  is odd and  $\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) < \nu_2(p_i - 1)$  (i.e.  $q$  does not generate the Sylow 2-subgroup of  $\mathbb{Z}_{p_i}^*$ ).*
- (iii)  *$n'_r$  is odd and  $q$  is a square of an element in  $\mathbb{Z}_{n'_r}$ .*

**Proof.** We refine Eq. (4.3) as follows:

$$\begin{aligned} P_{n,\lambda} &\stackrel{\text{CRT}}{=} (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}} \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}, \\ G_{n,r} &\stackrel{\text{CRT}}{=} (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}^*. \end{aligned} \quad (4.8)$$

(i) $\Rightarrow$ (ii). Let  $s$  be a multiplier of a Type-II duadic splitting  $P_{n,\lambda} = P_{n,\lambda}^{(0)} \cup P \cup sP$ . By Lemma 4.3(i),  $|1 + r\mathbb{Z}_{n_r r}| = |P_{n,\lambda}^{(0)}| = n_r$ . So

$$n - n_r = |P_{n,\lambda} \setminus P_{n,\lambda}^{(0)}| = |P| + |sP| = 2|P|,$$

which is an even integer. By the assumption of the theorem,  $n_r$  is odd. Thus  $n$  is odd, hence  $n'_r$  is odd. That is,  $p_i$  for  $i = 1, \dots, \ell$  are all odd.

Suppose that for some  $i$  the inequality in (ii) does not hold, without loss of generality, assume that  $p_1$  is odd and  $\nu_2(\text{ord}_{\mathbb{Z}_{p_1}^*}(q)) = \nu_2(p_1 - 1)$ . By Eq. (4.8), we write

$$s \stackrel{\text{CRT}}{=} (s_0, s_1, s_2, \dots, s_\ell) \in (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^* \times \mathbb{Z}_{p_2^{v_2}}^* \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}^*.$$

We assume that  $S$  is the Sylow 2-subgroup of  $\mathbb{Z}_{p_1^{v_1}}^*$ . Then  $|S| = 2^{\nu_2(p_1 - 1)}$ ,  $q$  generates  $S$ ,  $\mathbb{Z}_{p_1^{v_1}}^* = S' \times S$  for a subgroup  $S'$  of odd order, and

$$(1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^* = (1 + r\mathbb{Z}_{n_r r}) \times S' \times S$$

with  $(1 + r\mathbb{Z}_{n_r r}) \times S'$  being a direct factor of odd order. Thus, the quotient group

$$((1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^*) / \langle q \rangle_{(1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^*}$$

is of odd order, where  $\langle q \rangle_{(1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^*}$  is the subgroup of  $(1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}}^*$  generated by  $q$ . Hence, in the quotient group  $(s_0, s_1)$  is an element of odd order. Take

$$\alpha \stackrel{\text{CRT}}{=} (1, 1, 0, \dots, 0) \in (1 + r\mathbb{Z}_{n_r r}) \times \mathbb{Z}_{p_1^{v_1}} \times \mathbb{Z}_{p_2^{v_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{v_\ell}}.$$



Let  $Q_\alpha$  be the  $q$ -coset containing  $\alpha$ . Then  $\alpha \notin P_{n,\lambda}^{(0)}$  and  $Q_\alpha \subseteq P_{n,\lambda} \setminus P_{n,\lambda}^{(0)}$ . By Remark 2.2(iv), the length of the  $s$ -orbit on  $P_{n,\lambda}/\mu_q$  containing  $Q_\alpha$  is odd. Hence, by Remark 2.2(ii), the Type-II splittings of  $P_{n,\lambda}$  given by  $\mu_s$  do not exist. This is impossible because we have had a Type-II duadic splitting  $P_{n,\lambda} = P_{n,\lambda} \cup P \cup sP$  given by  $\mu_s$ . So the equality  $\nu_2(\text{ord}_{\mathbb{Z}_{p_1}^*}(q)) = \nu_2(p_1 - 1)$  has to be false.

(ii) $\Rightarrow$ (i). Assume that (ii) holds. By Eq. (4.6),  $\mathbb{Z}_{p_i}^{*v_i} = (1 + p_i\mathbb{Z}_{p_i}^{v_i}) \times H_i$  and the natural homomorphism

$$\mathbb{Z}_{p_i}^{*v_i} \rightarrow \mathbb{Z}_{p_i}^*, \quad k \pmod{p_i^{v_i}} \mapsto k \pmod{p_i}$$

induces an isomorphism  $H_i \cong \mathbb{Z}_{p_i}^*$ . The order of the kernel of the homomorphism is  $|1 + p_i\mathbb{Z}_{p_i}^{v_i}| = p_i^{v_i-1}$ , which is odd and coprime to the order  $|\mathbb{Z}_{p_i}^*| = p_i - 1$ . So

$$\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^{*v_i}}(t)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(t)), \quad \text{for any integer } t \text{ coprime to } p. \quad (4.9)$$

Then  $\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^{*v_i}}(q)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) < \nu_2(p_i - 1) = \nu_2(|\mathbb{Z}_{p_i}^{*v_i}|)$ . Since  $\mathbb{Z}_{p_i}^{*v_i}$  is a cyclic group, there is an  $s_i \in \mathbb{Z}_{p_i}^{*v_i}$  such that in the group  $\mathbb{Z}_{p_i}^{*v_i}$  we have  $s_i^2 = q$  and  $\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^{*v_i}}(s_i)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) + 1$ . By (4.9) again, we obtain that  $\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(s_i)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) + 1$ . So we get:

$$s_i \notin \langle q \rangle_{\mathbb{Z}_{p_i}^*} \quad \text{but} \quad s_i^2 \equiv q \pmod{p_i^{v_i}}, \quad i = 1, \dots, \ell. \quad (4.10)$$

By Eq. (4.8) we have an integer  $s$  as follows:

$$s \stackrel{\text{CRT}}{=} (1, s_1, \dots, s_\ell) \in (1 + r\mathbb{Z}_{n,r}) \times \mathbb{Z}_{p_1}^{*v_1} \times \dots \times \mathbb{Z}_{p_\ell}^{*v_\ell}.$$

By Eq. (4.10), in the quotient group  $G_{n,r}/\langle q \rangle_{G_{n,r}}$ , the element  $s$  has order 2, where  $\langle q \rangle_{G_{n,r}}$  stands for the subgroup of  $G_{n,r}$  generated by  $q$ .

Let  $Q$  be any  $q$ -coset on  $P_{n,\lambda}$  outside  $P_{n,\lambda}^{(0)}$ . We prove by contradiction that  $sQ \neq Q$ , which implies that the length of the  $\mu_s$ -orbit on  $P_{n,\lambda}/\mu_q$  containing  $Q$  is even (see Remark 2.2 (i) and (iv)), hence the statement (i) of the theorem holds, see Remark 2.2 (ii). Suppose that  $sQ = Q$ . Take any  $\mathbf{k} = (k_0, k_1, \dots, k_\ell) \in Q$  with

$$k_0 \in 1 + r\mathbb{Z}_{n,r}, \quad k_i \in \mathbb{Z}_{p_i}^{v_i} \quad \forall i = 1, \dots, \ell.$$

Then there is an integer  $d$  such that  $s\mathbf{k} = q^d\mathbf{k}$ . Since  $Q \cap P_{n,\lambda}^{(0)} = \emptyset$ , there is an  $m$  with  $1 \leq m \leq \ell$  such that  $k_m \not\equiv 0 \pmod{p_m^{v_m}}$ . But  $sk_m \equiv q^d k_m \pmod{p_m^{v_m}}$ . By the argument for Eq. (4.7), we have  $s \equiv q^d \pmod{p_m}$ , which implies that  $s_m \in \langle q \rangle_{\mathbb{Z}_{p_m}^*}$ . That is a contradiction to Eq. (4.10).

(ii) $\Rightarrow$ (iii). Taking  $s' \in \mathbb{Z}_{n_r}^*$  such that  $s' \stackrel{\text{CRT}}{=} (s_1, \dots, s_\ell) \in \mathbb{Z}_{p_1}^{*v_1} \times \dots \times \mathbb{Z}_{p_\ell}^{*v_\ell}$  where  $s_i$  for  $i = 1, \dots, \ell$  are taken in Eq. (4.10), we obtain  $s'^2 \equiv q \pmod{n'_r}$ .

(iii) $\Rightarrow$ (ii). Assume that  $s'^2 \equiv q \pmod{n'_r}$ . For  $p_i$  with  $i = 1, \dots, \ell$ , we have  $s'^2 \equiv q \pmod{p_i}$ . If  $\text{ord}_{\mathbb{Z}_{p_i}^*}(s')$  is odd, then  $\text{ord}_{\mathbb{Z}_{p_i}^*}(q)$  is odd, hence  $\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) = 0 < \nu_2(p_i - 1)$ . Otherwise,  $\text{ord}_{\mathbb{Z}_{p_i}^*}(s')$  is even, hence

$$\nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(q)) = \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(s'^2)) < \nu_2(\text{ord}_{\mathbb{Z}_{p_i}^*}(s')) \leq \nu_2(p_i - 1).$$

The proof of the theorem is finished.  $\square$

In the extreme case where  $n_r = 1$  (whether  $r = 1$  or not),  $n = n'_r$  and Eq. (4.3) becomes

$$\begin{aligned} P_{n,\lambda} &\stackrel{\text{CRT}}{=} \{1\} \times \mathbb{Z}_n \cong \mathbb{Z}_n, \\ G_{n,r} &\stackrel{\text{CRT}}{=} \{1\} \times \mathbb{Z}_n^* \cong \mathbb{Z}_n^*. \end{aligned}$$

Thus, we can view even-like duadic cyclic codes as a special case of Type-II (even-like) duadic constacyclic codes.

**Corollary 4.7** ([15, Theorem 6.3.2]). *Even-like (i.e., Type-II) duadic cyclic codes of length  $n$  over  $F_q$  exist if and only if  $n$  is odd and  $q$  is a square of an element in  $\mathbb{Z}_n$ .*

## 5 Examples

We show that some good codes can be constructed from Type-II (even-like) duadic constacyclic codes.

**Proposition 5.1.** *Assume that  $\nu_2(q-1) \geq 2$  (equivalently,  $\nu_2(q+1) = 1$ ). Let  $n = q+1 = 2n'$ ,  $r = 2^{\nu_2(q-1)}$ ,  $r' = \frac{q-1}{r}$  and  $s = 1 + rn'$ . Let*

$$P = \left\{ 1 + ri \mid \frac{n' + r'}{2} < i < \frac{3n' + r'}{2} \right\} \subseteq P_{n,\lambda} = 1 + r\mathbb{Z}_{nr}.$$

*Then  $P$  is  $\mu_q$ -invariant and  $C_P, \varphi_s(C_P)$  are a pair of even-like  $\lambda$ -constacyclic codes of length  $n$ , which are alternant codes over  $F_q$  from generalized Reed-Solomon codes over  $F_{q^2}$ ; in particular, they are  $[q+1, \frac{q-1}{2}, \frac{q+5}{2}]$  MDS-codes.*

**Proof.** Denote  $e = \nu_2(q-1) \geq 2$ . Note that  $n_r = 2$ ,  $n'_r = n'$  is odd and  $q = 1 + rr' = 1 + 2^e r'$  with  $r'$  being odd. So  $q$  generates the group  $1 + r\mathbb{Z}_{n_r r} = 1 + 2^e \mathbb{Z}_{2e+1}$ . In particular, Type-I duadic  $\lambda$ -constacyclic codes of length  $n$  over  $F_q$  do not exist, cf. Lemma 4.3 (iii).

Since  $0 < r' = \frac{q-1}{2^e} < \frac{q+1}{2} = n'$ , we have

$$r' < \frac{n' + r'}{2} < n' < \frac{n' + r'}{2} + n' = \frac{3n' + r'}{2} < n.$$

And  $|P| = n' - 1$ . Since  $\frac{r'}{2} + 1 = \frac{q-1}{2} + 1 = n'$ ,

$$1 + r \frac{n' + r'}{2} = \frac{r}{2} n' + \frac{rr'}{2} + 1 = \left(\frac{r}{2} + 1\right) n'.$$

And  $\frac{3n'+r'}{2} = \frac{n'+r'}{2} + n'$ . By Eq. (3.4),

$$P_{n,\lambda}^{(0)} = \{1 + r\frac{n'+r'}{2}, 1 + r\frac{3n'+r'}{2}\}.$$

For any  $1 + ri \in P_{n,\lambda}$ , noting that  $q = 1 + rr' = n - 1$ , we have

$$\begin{aligned} q(1 + ri) &= q + qri = 1 + rr' + nri - ri \\ &\equiv 1 + r(r' - i) \equiv 1 + r(n + r' - i) \pmod{nr}. \end{aligned}$$

If  $\frac{n'+r'}{2} < i < \frac{3n'+r'}{2}$ , it is easy to check that

$$\frac{n'+r'}{2} < n + r' - i < \frac{3n'+r'}{2}.$$

Thus, the subset  $P$  is  $\mu_q$ -invariant. Next we compute

$$\begin{aligned} s(1 + ri) &= (1 + rn')(1 + ri) = 1 + r(n' + i) + \frac{r}{2}nri \\ &\equiv 1 + r(n' + i) \pmod{nr}. \end{aligned}$$

Since  $P$  consists of the points  $1 + ri$  with  $i$  running from  $\frac{n'+r'}{2} + 1$  to  $\frac{n'+r'}{2} + n' - 1$  consecutively, we obtain that  $P \cap sP = \emptyset$ . As  $|P_{n,\lambda}| = 2n' = |P_{n,\lambda}^{(0)}| + |P| + |sP|$ , we further obtain that  $P = P_{n,\lambda}^{(0)} \cup P \cup sP$ . In conclusion,  $C_P$  and  $\varphi_s(C_P)$  are a pair of even-like duadic  $\lambda$ -constacyclic codes over  $F_q$ .

Because  $nr$  is a divisor of  $(q + 1)(q - 1) = q^2 - 1$ , in the extension  $F_{q^2}$  of  $F_q$  we can take a primitive  $nr$ -th root  $\theta$  of unity such that  $\theta^n = \lambda$ . By  $\tilde{C}_P$ ,  $\varphi_s(\tilde{C}_P)$  we denote the pair of even-like duadic  $\lambda$ -constacyclic codes over  $F_{q^2}$ . It is clear that  $C_P = \tilde{C}_P|_{F_q}$  is the subfield subcode from  $\tilde{C}_P$ . It is the same for  $\varphi_s(C_P)$ .

Let  $\hat{C} = \{\mathbf{c}_f \mid f = f(X) \in F_{q^2}[X], \deg f < n' - 1\} \subseteq F_{q^2}^{n'}$  with

$$\mathbf{c}_f = (f(1), \theta^{-(rz+1)}f(\theta^{-r}), \dots, \theta^{-(rz+1)(n-1)}f(\theta^{-r(n-1)})) \in F_{q^2}^{n'},$$

where  $z = \frac{n'+r'}{2} + 1$ . Then  $\hat{C}$  is a generalized Reed-Solomon code. To complete the proof of the proposition, it is enough to show that  $\tilde{C}_P = \hat{C}$ .

Any codeword  $\mathbf{c}_f$  of  $\hat{C}$  for  $f(X) = \sum_{k=0}^{n'-2} f_k X^k$  corresponds to the following  $F_{q^2}$ -polynomial

$$c_f(X) = \sum_{j=0}^{n-1} \theta^{-(rz+1)j} f(\theta^{-rj}) X^j = \sum_{j=0}^{n-1} \theta^{-(rz+1)j} \sum_{k=0}^{n'-2} f_k \theta^{-rjk} X^j.$$

Let  $1 + rm \in \bar{P} = P_{n,\lambda} \setminus P$ , i.e.,  $0 \leq m < z$  or  $z + n' - 1 \leq m < n$ . Note that  $\theta^{-r}$  is a primitive  $n$ -th root of unity. For any  $i$  with  $z \leq i \leq z + n' - 2$ , we have

$\theta^{-r(i-m)} \neq 1$ . Then

$$\begin{aligned}
c_f(\theta^{1+rm}) &= \sum_{j=0}^{n-1} \sum_{k=0}^{n'-2} \theta^{-(rz+1)j} f_k \theta^{-rjk} \theta^{(1+rm)j} \\
&= \sum_{k=0}^{n'-2} f_k \sum_{j=0}^{n-1} \theta^{-r(z+k-m)j} \\
&= \sum_{k=0}^{n'-2} f_k \cdot \frac{\theta^{-r(z+k-m)n} - 1}{\theta^{-r(z+k-m)} - 1} = 0.
\end{aligned}$$

Since  $\overline{P}$  is the defining set of  $\tilde{C}_P$ , we get that  $c_f(X) \in \tilde{C}_P$ , see Remark 2.1. Thus  $\hat{C} \subseteq \tilde{C}_P$ . This inclusion has to be an equality because the dimensions of the two hand sides are equal to each other.  $\square$

The following is a specific numerical example of Proposition 5.1.

**Example 5.2.** Take  $q = 13$ ,  $n = 14$ ,  $r = 4$  (i.e.,  $\lambda = 5$ ). Then  $n_r = 2$ ,  $n' = n'_r = 7$ ,  $nr = 56$  and

$$P_{n,\lambda} = \{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53\},$$

which is partitioned into  $q$ -cosets as follows:

$$\begin{aligned}
Q_0 &= P_{n,\lambda}^{(0)} = \{21, 49\}, \\
Q_1 &= \{1, 13\}, \quad Q_2 = \{5, 9\}, \quad Q_3 = \{17, 53\}, \\
Q_4 &= \{25, 45\}, \quad Q_5 = \{29, 41\}, \quad Q_6 = \{33, 37\};
\end{aligned}$$

and  $\prod_{i \in P_{n,\lambda}^{(0)}} (X - \theta^i) = X^2 + 5$ . Take  $s = 1 + rn' = 29$ , then  $s^2 \equiv 1 \pmod{56}$ . Then  $\mu_s$  permutes the quotient set  $P_{n,\lambda}/\mu_q$  of  $q$ -cosets into four orbits as follows:

$$(Q_0)(Q_1, Q_5)(Q_2, Q_6)(Q_3, Q_4).$$

Let

$$P = Q_4 \cup Q_5 \cup Q_6 = \{25, 29, 33, 37, 41, 45\};$$

then

$$sP = Q_1 \cup Q_2 \cup Q_3 = \{1, 5, 9, 13, 17, 53\}.$$

Obviously,

$$P_{n,\lambda}^{(0)} \cup P \cup sP = P_{n,\lambda}, \quad P_{n,\lambda}^{(0)} \cap P = P_{n,\lambda}^{(0)} \cap sP = P \cap sP = \emptyset.$$

Thus  $C_P$ ,  $C_{sP}$  are a pair of even-like duadic  $\lambda$ -constacyclic codes over  $F_{13}$  with parameters  $[14, 6, 9]$ .

Finally we exhibit an example where  $n_r$  is odd.

**Example 5.3.** Take  $q = 4$ ,  $n = 21$ ,  $r = 3$  hence  $F_4 = \{0, 1, \lambda, \lambda^2\}$ . Then  $n_r = 3$ ,  $n'_r = 7$ ,  $nr = 63$  and

$$P_{n,\lambda} = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61\},$$

which is partitioned into  $q$ -cosets as follows:

$$\begin{aligned} Q_0 &= P_{n,\lambda}^{(0)} = \{7, 28, 49\}, \\ Q_1 &= \{1, 4, 16\}, \quad Q_2 = \{10, 40, 34\}, \quad Q_3 = \{13, 52, 19\}, \\ Q_4 &= \{22, 25, 37\}, \quad Q_5 = \{31, 61, 55\}, \quad Q_6 = \{43, 46, 58\}; \end{aligned}$$

and

$$\prod_{i \in P_{n,\lambda}^{(0)}} (X - \theta^i) = X^3 - \lambda.$$

Since  $5^2 \equiv 4 \pmod{7}$ , even-like duadic  $\lambda$ -constacyclic codes exist. Take  $s = 55 \equiv -8 \pmod{63}$ , then  $s^2 \equiv 1 \pmod{63}$ . Then  $\mu_s$  permutes the quotient set  $P_{n,\lambda}/\mu_q$  of  $q$ -cosets into four orbits as follows:

$$(Q_0)(Q_1, Q_5)(Q_2, Q_6)(Q_3, Q_4).$$

Let

$$P = Q_1 \cup Q_2 \cup Q_3 = \{1, 4, 10, 13, 16, 19, 34, 40, 52\};$$

then

$$sP = Q_4 \cup Q_5 \cup Q_6 = \{22, 25, 31, 37, 43, 46, 55, 58, 61\}.$$

Obviously,

$$P_{n,\lambda}^{(0)} \cup P \cup sP = P_{n,\lambda}, \quad P_{n,\lambda}^{(0)} \cap P = P_{n,\lambda}^{(0)} \cap sP = P \cap sP = \emptyset.$$

Thus  $C_P$ ,  $C_{sP}$  are a pair of even-like duadic  $\lambda$ -constacyclic codes over  $F_4$  with parameters  $[21, 9, d]$ , where the minimum distance  $d \geq 8$  since the defining set of  $C_{sP}$  is

$$P_{n,\lambda} \setminus sP = P_{n,\lambda}^{(0)} \cup P = \{1, 4, 7, 10, 13, 16, 19, 28, 34, 40, 49, 52\},$$

which contains 7 consecutive points 1, 4, 7, 10, 13, 16, 19 of  $P_{n,\lambda}$ .

## Acknowledgements

The research of the authors is supported by NSFC with grant number 11271005. It is the authors' pleasure to thank the anonymous referees for their helpful comments which led to improvements of the paper.

## References

- [1] J. L. Alperin, R. B. Bell, Groups and Representations, GTM 162, Springer-Verlag, New York, 1997.
- [2] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, Duadic group algebra codes, In Proc. Int. Symp. Inf. Theory, Adelaide, Australia, (2007), 2096-2100.
- [3] N. Aydin, I. Siap, D. J. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr., **24**(2001), 313-326.
- [4] T. Blackford, Negacyclic duadic codes, Finite Fields Appl., **14**(2008), 930-943.
- [5] T. Blackford, Isodual constacyclic codes, Finite Fields Appl., **24**(2013), 29-44.
- [6] R. A. Brualdi, V. Pless, Polyadic codes, Discr. Appl. Math., **25**(1989), 3-17.
- [7] Bocong Chen, H. Q. Dinh, Yun Fan, San Ling, Polyadic constacyclic codes, IEEE Trans. Inform. Theory **61**(2015), no.9, 4895-4904.
- [8] Bocong Chen, Yun Fan, Liren Lin, Hongwei Liu, Constacyclic codes over finite fields, Finite Fields Appl., **18**(2012), 1217-1231.
- [9] H. Q. Dinh, Repeated-root constacyclic codes of length  $2ps$ , Finite Fields Appl. **18** (2012) 133-143.
- [10] H. Q. Dinh, Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory **50**(2004), no.8, 1728-1744.
- [11] C. Ding, V. Pless, Cyclotomy and duadic codes of prime lengths, IEEE Trans. Inform. Theory, **45**(1999), 453-466.
- [12] C. Ding, K.Y. Lam, C. Xing, Enumeration and construction of all duadic codes of length  $p^m$ , Fund. Inform. **38**(1999), 149-161.
- [13] Yun Fan, Guanghui Zhang, On the existence of self-dual permutation codes of finite groups, Des. Codes Cryptogr., **62**(2012), 19-29.
- [14] S. Han, J-L. Kim, Computational results of duadic double circulant codes, J. Appl. Math. Comput., **40**(2012), 33-43.
- [15] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
- [16] J. S. Leon, J. M. Masley, V. Pless, Duadic codes, IEEE Trans. Inform. Theory, **30**(1984), 709-714.
- [17] V. Pless, Duadic codes revisited, Congressus Numeratium, **59**(1987), 225-233.

- [18] J. J. Rushanan, Duadic codes and difference sets, J. Combin. Theory Set. A, **57**(1991), 254-61.
- [19] M. H. M. Smid, Duadic codes, IEEE Trans. Inform. Theory, **33**(1987), 432-433.
- [20] H. N. Ward, L. Zhu, Existence of abelian group codes partitions, J. Combin. Theory Ser. A, **67**(1994), 276-281.